POWERED BY Dialog

Management of application program loaded into microcircuit - usingpre-generated coded key stored in programmable memory for comparison withcode generated as program runs to enable smart-card function

Patent Assignee: GERONIMI F; GEMPLUS CARD INT SA
Inventors: GERONIMI F; GERONIMIF

Patent Family

Patent Number	Kind	Date	Application Number	Kind	Date	Week	Type
EP 475837	A	19920318	EP 91402408	A	19910910	199212	B
FR 2666671	A	19920313	FR 9011293	A	19900912	199219	
CA 2051365	A	19920313	CA 2051365	A	19910913	199221	
US 5191608	A	19930302	US 91757726	A	19910911	199311	
EP 475837	B1	19930811	EP 91402408	A	19910910	199332	
DE 69100256	E	19930916	DE 600256	A	19910910	199338	
			EP 91402408	A	19910910		
CA 2051365	C	19960220	CA 2051365	A	19910913	199618	N

Priority Applications (Number Kind Date): FR 9011293 A (19900912)
Cited Patents: 1. journal ref.; EP 299826 ; EP 30381 ; FR 2503423

Patent Details

Patent	Kind	Language	Page	Main IPC	Filing Notes
EP 475837	A		10		
Designated States (Regional): DE ES FR GB IT NL					
CA 2051365	A	F		G06K-019/073	
US 5191608	A		6	H04L-009/00	
EP 475837	B1	F	10	G07F-007/10	
Designated States (Regional): DE ES FR GB IT NL					
DE 69100256	E			G07F-007/10	Based on patent EP 475837
CA 2051365	C	F		G06K-019/073	

Abstract:
EP 475837 A

The program is loaded into a microcircuit that is part of a smart card, and operates in several stages. Initially a coded signature is generated from a secret code (10) in the microcircuit and from instructions in the program (12). This signature is loaded into a programmable memory (14) in the microcircuit. The

microprocessor in the microcircuit generates another coded signature during execution of the application program.

The two signatures are compared and the continuation of the program is authorised if they coincide.

USE/ADVANTAGE - As smart cart for banking. Simplified program management for multiple applications incorporated into single smart card.

Dwg.1/2

EP 475837 B

A method for the management of an application program loaded in a microcircuit-based medium (2), comprising the following steps:

(a) to load the application program:

- an encrypted signature is prepared as a function of a secret code (10) of the microcircuit and certain instructions of the program;

- this signature if loaded into a programmable memory (14) of the microcircuit;

- the program is loaded into a program memory (12) of the microcircuit;

(b) when the application program is to be executed:

- before the execution of the application program, the microprocessor of the microcircuit is made to prepare (11) another encrypted signature;

- this signature is compared (17, 18); and

- the program is allowed to run on according to the result of this comparison.

Dwg.1/2

US 5191608 A

The application program management method involves computing a signature according to complex encrypting algorithm taking account, firstly, of a secret code proper to the card and, secondly, of the instructions proper to the program.

The signature thus computed is compared with a signature that has been pre-recorded in the card under the same conditions at the time of its delivery by the card-issuing party. It is shown that several uses can be authorised without jeopardising their security.

USE - For chip cards.

Dwg.2/2

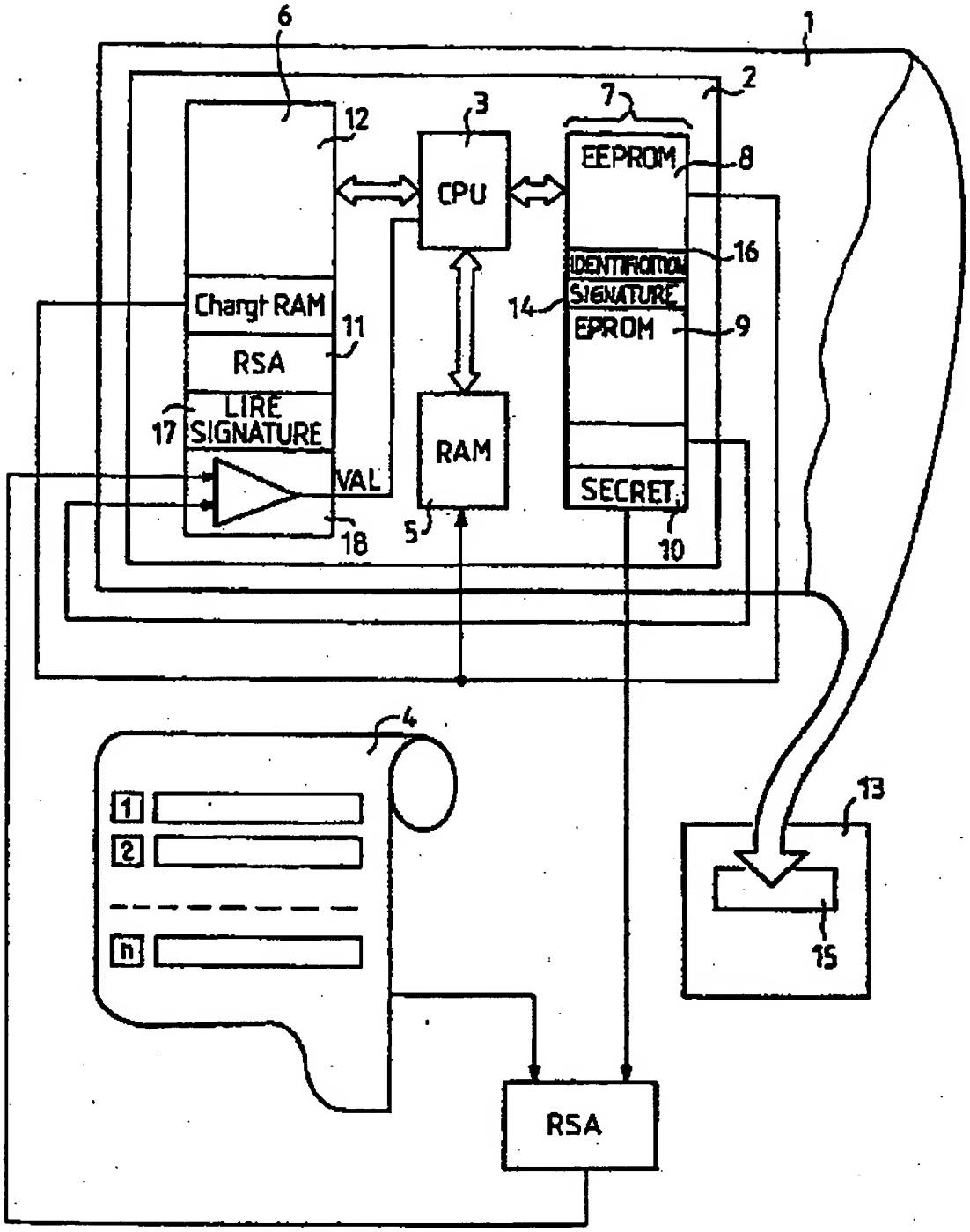

FIG_1

Derwent World Patents Index
© 2004 Derwent Information Ltd. All rights reserved.
Dialog® File Number 351 Accession Number 8963145